National Infrastructure Protection Center
CyberNotes

Issue #2000-15 *July 31, 2000*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, hacker exploit scripts, hacker trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between July 14 and July 27, 2000. The table provides the hardware/operating system, equipment/software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear as red and/or italic text.** Where applicable, the table lists a "CVE number" which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Adobe[1] Windows 95/98/NT 4.0/2000	Acrobat Reader 3.0, 4.0, 4.05; Acrobat Business Tools 4.0, 4.05; Acrobat 3.0, 4.0, 4.05	An exploitable buffer overflow vulnerability exists when reading a PDF file, which could cause the application to crash or allow the execution of arbitrary code.	Patch available at: ftp://ftp.adobe.com/pub/adobe/acrobat/win/4.x/ac405up2.exe	Adobe Acrobat Reader Business Tools Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[1] Shadow Penguin Security, SPS Advisory #39, July 26, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
AnalogX[2] Windows	Proxy 4.04	Many of the services that are provided by Proxy 4.04 contain buffer overflow vulnerabilities that can allow a remote malicious user to crash the proxy server.	Download Proxy 4.05 available at: http://www.analogx.com/contents/download/network/proxy.htm	Proxy Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
AnalogX[3] Windows 95/98/NT 4.0	SimpleServer: WWW 1.0.6	SimpleServer is vulnerable to a relative directory path attack that allows a remote malicious user to retrieve any known file from the file system of the server on which it is hosted.	Download SimpleServer:WWW version 1.07 from: http://www.analogx.com/contents/download/network/sswww.htm	SimpleServer WWW Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Blackboard[4] Windows NT 4.0, Unix	CourseInfo for Unix, CourseInfo 4.0	A vulnerability exists which could allow any user, with a valid account, the ability to modify the database by entering custom form values through any Perl script located in /bin and its subdirectories.	Version 5.0 of CourseInfo (now called Blackboard) is not susceptible to this vulnerability and is available at: http://download.blackboard.com	CourseInfo Database Modification	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Conectiva[5] Unix	OpenLDAP 1.2.7, 1.2,78, 1.2.9, 1.2.10, 1.2.11	The Interactive LDAP Directory Server query program, UD, could possibly be used to elevate privileges.	Users should upgrade to new packages or at least remove the reference to klogd in /etc/logrotate.d/openldap. ftp://ftp.conectiva.com.br/pub/conectiva/atualizacoes/	OpenLDAP UD Group Writable	Medium	Bug discussed in newsgroups and websites.
CVSWeb Developer[6] Windows NT 2000, Unix	CVSWeb 1.80	A vulnerability exists that provides malicious users, who have write access to a CVS repository, the ability to execute arbitrary commands on the host machine.	Upgrade to version 1.86 or higher, available at: http://stud.fh-heilbronn.de/~zeller/cgi/cvsweb.cgi/	CVSWeb Insecure Perl	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
GAMSoft[7] Windows 95/98/NT 4.0/2000	Telsrv 1.4, 1.5	A remote Denial of Service vulnerability exists when a malicious user submits an overly long user name, causing the service to stop responding.	No workaround or patch available at time of publishing.	Telsrv Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.

[2] Foundstone, Inc. Security Advisory, FS-072500-7-ANA, July 25, 2000.
[3] Foundstone, Inc. Security Advisory, FS-072600-8-ANA, July 26, 2000.
[4] Bugtraq, July 18, 2000.
[5] Conectiva Linux Security Announcement, 2000-07-26:ldap, July 26, 2000.
[6] Securiteam, July 20, 2000.
[7] Securiteam, July 17, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Hewlett-Packard[8]	JetDirect J3111A rev. A.08.06, G.05.35, G.07.02, G.07.03, G.07.17, G.08.03, JetDirect rev. G.08.04, G.08.20, H.08.05, H.08.20	A Denial of Service vulnerability exists due to the FTP service, which fails to properly handle bad FTP commands.	A fix for this vulnerability will be implemented in the next firmware revision for HP JetDirect print servers.	HP JetDirect Invalid FTP Command Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
IBM[9] Windows NT, Unix	WebSphere 3.0.2	A show code vulnerability exists, which could allow a malicious user to view the source code of any file within the web document root of the web server.	Patch available at: http://www-4.ibm.com/software/webservers/appserv/efix.html	IBM WebSphere Showcode	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Infopulse[10] Windows 95/98/NT 4.0/2000	GateKeeper 3.5 and previous	An exploitable buffer overflow vulnerability exists, which could allow a remote malicious user to execute arbitrary code on the server.	Upgrade to version 3.6, which is not susceptible to this vulnerability.	Gatekeeper Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.
ITAfrica[11] Windows 95/98/NT 4.0/2000	WEBactive 1.0	A remote Denial of Service vulnerability exists when an URL with 280+ characters is requested.	No workaround or patch available at time of publishing. **This product is no longer in production.**	WEBactive HTTP Server Long GET Request	Low	Bug discussed in newsgroups and websites. Exploit has been published.
L-Soft[12] Windows 9x/2000/ NT 3.5x/4.0, Unix, OpenVMS VAX	Listserv 1.8c, 1.8d	An unchecked buffer overflow vulnerability exists in the web archive (wa, wa.exe) component, which could allow remote execution of arbitrary code with the privileges of the LISTSERV daemon.	Patches for version 1.8d are available from L-Soft. (Patches are not available for 1.8c, which is no longer supported.) http://www.lsoft.com/news/default.asp?item=Advisory1	Listserv Web Archives Long QUERY_ STRING Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
MandrakeSoft Linux[13] Unix	Mandrake 7.1	A vulnerability exists in the usermode package that permits malicious users to reboot or halt the system without having root access.	Update available at: ftp://ftp.linux.tucows.com/pub/distributions/Mandrake/Mandrake/updates	Linux Usermode Package	Low	Bug discussed in newsgroups and websites.

[8] VIGILANTE-2000004, July 19, 2000.
[9] Foundstone, Inc. Security Advisory, FS-072400-6-IBM, July 23, 2000.
[10] Securiteam, July 18, 2000.
[11] Securiteam, July 17, 2000.
[12] Network Associates, Inc. COVERT Labs Security Advisory, COVERT-2000-07, July 17, 2000.
[13] Linux-Mandrake Security Update Advisory, MDKSA-2000:020, July 18, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft[14] Windows 95/98/NT 4.0/2000	Internet Explorer 5.01, 5.5 (also affects Microsoft Outlook)	A security vulnerability exists that enables malicious web sites to create a special HTML page which reads the content of any local and remotely accessible HTML or text file. Furthermore, the ability to read parsed web pages from Intranet web servers, who are supposedly secured behind the firewall, exists. This vulnerability is also exploitable from HTML based e-mail messages.	**Unofficial Workaround:** **(Georgi Guninski)** Disable Active Scripting or disable Run ActiveX controls and plug-ins.	Internet Explorer DHTMLED and IFRAME File Read	Medium / **High**	Bug discussed in newsgroups and websites. Exploit has been published. Vulnerability has appeared in the Press and other public media
Microsoft[15] Windows NT 4.0/2000	Internet Information Server (IIS) 2.0, 3.0, 4.0, 5.0	Under particular conditions, IIS will disclose its internal IP address in the authentication realm parameter if an HTTP 1.0 request is made to a restricted directory using basic authentication.	Changing the w3svc/UseHostName value in the metabase from False to True can alter this behavior. Detailed instructions can be found in the Microsoft knowledge base at: http://support.microsoft.com/support/kb/articles/Q218/1/80.ASP	Internet Information Server IP Address Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[16] **Windows 95/98/NT 4.0/2000** ***Microsoft issues patch.[17]***	**Excel 97, 2000**	**A vulnerability exists in the REGISTER.ID function, which allows the execution if programs when opening an Excel Workbook (.xls file). This may be also be exploited through Internet Explorer or Outlook and may enable malicious users to take full control over the target's computer by installing a Trojan on the computer and then executing it.**	**No workaround or patch available at time of publishing.** ***Frequently asked questions regarding this vulnerability and the patch can be found at:*** http://www.microsoft.com/technet/security/bulletin/fq00-051.asp	**Excel 97/2000 Register.ID**	**High**	**Bug discussed in newsgroups and websites. Exploit has been published.** **Vulnerability has appeared in the Press and other public media.**

[14] Georgi Guninski Security Advisory #16, July 14, 2000.
[15] Security Alert Consensus #054, July 20, 2000.
[16] Georgi Guninski Security Advisory #15, July 11, 2000.
[17] Microsoft Security Bulletin, MS00-051, July 26, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft[18] Windows NT 4.0/2000	Internet Information Server (IIS) 4.0, 5.0	Two security vulnerabilities exist which could allow a malicious user to stop the server from providing useful service, or to extract certain types of information from it.	**IIS 4.0:** http://www.microsoft.com/Downloads/Release.asp?ReleaseID=22709 **IIS 5.0:** http://www.microsoft.com/Downloads/Release.asp?ReleaseID=22708 **Note:** Customers who choose to install the patch should also strengthen the permissions on the /scripts/iisadmin folder in each web site on the server, and ensure that only administrators can access it.	Internet Information Server Directory Browser Argument	Medium	Bug discussed in newsgroups and websites.
Microsoft[19] Windows 95/98/NT 4.0/2000	Outlook Express 4.0, 4.01, 5.0, 5.01	A security vulnerability exists which could allow a malicious user to send an e-mail that would "read over the shoulder" of the recipient as he/she previews subsequent e-mails in Outlook Express.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq00-045.asp **Note**: In addition to eliminating the vulnerability, customers who already have taken the corrective action discussed in Microsoft Security Bulletins MS00-043 and MS00-046 do not need to take any additional action.	Outlook Express Persistent Mail-Browser Link	Medium	Bug discussed in newsgroups and websites.
Microsoft[20] Windows 95/98/NT 4.0/2000	Outlook Express 4.0, 4.01, 5.0, 5.01, Outlook 97.0, 98, 2000	A security vulnerability exists, which could allow a malicious user to send an HTML mail that, when opened, could read, but not add, change or delete, files on the recipient's computer. If coupled with other vulnerabilities, it could potentially be used in more advanced attacks as well.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq00-046.asp **Note:** In addition to eliminating the vulnerability, customers who already have taken the corrective action discussed in Microsoft Security Bulletins MS00-043 and MS00-045do not need to take any additional action.	Outlook / Outlook Express Cache Bypass	Medium	Bug discussed in newsgroups and websites.
Microsoft[21] Windows 95/98/NT 4.0	Outlook Express 4.0, 4.01, 5.0, 5.01; Outlook 97.0, 98, 2000;	A component shared by Outlook and Outlook Express contains a buffer overflow vulnerability, which could let a malicious user crash the system reading the e-mail or run arbitrary code. **Note:** The buffer overflow can occur even if the user does not open or preview the e-mail message.	Frequently asked questions regarding this vulnerability and the patch can be found at http://www.microsoft.com/technet/security/bulletin/fq00-043.asp **Note:** In addition to eliminating the vulnerability, customers who already have taken the corrective action discussed in Microsoft Security Bulletins MS00-046 and MS00-045 do not need to take any additional action.	Outlook / Outlook Express Malformed E-mail Header	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published. Vulnerability has appeared in the Press and other public media.

[18] Microsoft Security Bulletin, MS00-044, July 14, 2000.
[19] Microsoft Security Bulletin, MS00-045, July 20, 2000.
[20] Microsoft Security Bulletin, MS00-046, July 20, 2000.
[21] Microsoft Security Bulletin, MS00-043, July 20, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft[22] **Windows NT 2000** ***Corrected version of patch released.[23]***	**Windows NT 2000**	**A security vulnerability exists which could make it easier for a malicious user who had complete control over a Windows 2000 machine to compromise users' sensitive information.** ***Updated to correct a packaging and regression problem with the original patch.***	**Patch available at:** **http://download.microsoft.com/download/win2000platform/Update/Q260219/NT5/EN-US/Q260219_W2K_SP1_x86_en.EXE** ***Updated Patch:*** **http://www.microsoft.com/Downloads/Release.asp?ReleaseID=23332**	**Microsoft Windows 2000 Protected Store Key Length**	**High**	**Bug discussed in newsgroups and websites.**
Microsoft[24] Windows NT 4.0/2000	Windows NT 4.0 Workstation, Server, Enterprise Edition, Terminal Server Edition, Windows 2000	The Microsoft Windows implementation of NetBIOS allows an unsolicited UDP datagram to remotely deny access to services offered by registered NetBIOS names. A malicious user can remotely shut down all Domain Logins, the ability to access SMB shares, and NetBIOS name resolution services.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq00-047.asp	Windows NT NetBIOS Name Server Protocol Spoofing	Medium	Bug discussed in newsgroups and websites.
Microsoft[25] Windows NT 4.0/2000	Windows NT 4.0, 2000	When executables and DLL files are not preceded by a path in the registry, this could open up the possibility of automatic execution of Trojans if they are renamed as executables that do not have a path specified.	**Unofficial Workaround (Bugtraq):** Verify that that all executable file names in the registry have a path specified. You also can move a copy of real explorer.exe to the system drive root directory and grant specific rights.	Windows NT Unspecified Executable Path	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[26] **Windows NT 2000** ***Microsoft issues patch.[27]***	**Windows NT 2000, 2000.2072, 2000.2031, 2000.0.2195**	**A Denial of Service vulnerability exists in the Telnet server, which may be exploited by a local or remote attacker.**	**No workaround or patch available at time of publishing.** ***Frequently asked questions regarding this vulnerability and the patch can be found at:*** **http://www.microsoft.com/technet/security/bulletin/fq00-050.asp**	**Windows 2000 Telnet Server Denial of Service**	**Low**	**Bug discussed in newsgroups and websites. Exploit has been published.**

[22] Microsoft Security Bulletin, MS00-032, June 2, 2000.
[23] Microsoft Security Bulletin, MS00-032, July 26, 2000.
[24] Microsoft Security Bulletin, MS00-047, July 27, 2000.
[25] Bugtraq, July 26, 2000.
[26] SecureXpert Labs Advisory, SX-20000620-1, June 30, 2000.
[27] Microsoft Security Bulletin, MS00-050, July 24, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Multiple Vendors[28] Unix	Conectiva Linux 4.0-4.2, 5.0; Debian Linux 2.2, 2.3; RedHat Linux 6.0-6.3; Trustix Secure Linux 1.0, 1.1	A vulnerability exists in the rpc.statd daemon, which could let remote malicious users gain root access to the system or could cause the rpc.statd program to execute arbitrary code.	Contact your vendor for update	Multiple Vendor Rpc.statd Remote Format String Stack Overwrite	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Multiple Vendors[29, 30] Unix	Conectiva Linux 4.0-4.2, 5.0-5.1; RedHat Linux 6.0-6.2 alpha, i386, sparc	A vulnerability exists in the Linux pam_console module that could potentially allow remote malicious users to access console devices and shut down the workstation if the workstation is running a display manager (xdm, gdm, kdm, etc.) with XDMCP enabled.	**Conectiva Linux 5.1:** ftp://ftp.conectiva.com.br/pub/conectiva/atualizacoes/4.0/i386/pam-0.72-15cl.i386.rpm **RedHat Linux:** RedHat upgrade RHSA-2000:044-02 Updated pam packages located at: http://www.redhat.com/support/errata/RHSA-2000-044-02.html	Multiple Linux Vendor pam Remote User	Medium	Bug discussed in newsgroups and websites.
Multiple Vendors[31, 32, 33] Unix	Conectiva Linux 4.0-4.2, 5.0-5.1; OpenLinux eDesktop 2.4, OpenLinux eServer 2.3 and OpenLinux eBuilder, OpenLinux Desktop 2.3; Red Hat Linux 5.2 and 6.x	A vulnerability exists in the GPM (General Purpose Mouse) package, which could allow a malicious user to remove arbitrary files.	**Conectiva Linux:** All users should upgrade. This upgrade also requires an updated version of the PAM package, available at: ftp://ftp.conectiva.com.br/pub/conectiva/atualizacoes/ **Caldera Systems:** The upgrade packages can be found on Caldera's FTP site at: ftp://ftp.calderasystems.com/pub/updates/OpenLinux/2.3/current/RPMS/ **RedHat Linux:** For 6.x, the /dev/gpmctl ownership issue was addressed via the pam_console helper mechanism. This pam module makes devices, which need to be accessible via console users owned by them and no one else. See RHSA-2000:044 for more information on this update.	Linux GPM File Removal	Medium	Bug discussed in newsgroups and websites.

[28] Security Alert Consensus #054, July 20, 2000.
[29] Conectiva Linux Security Announcement, 2000-07-28:pam, July 27, 2000.
[30] Red Hat, Inc. Security Advisory, RHSA-2000:044-02, July 21, 2000.
[31] Conectiva Linux Security Announcement, 2000-07.27:gpm, July 27, 2000.
[32] Caldera Systems, Inc. Security Advisory, CSSA-2000-024.0, July 6, 2000.
[33] Red Hat, Inc. Security Advisory, RHSA-2000:045-01, July 26, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Netscape[34]	Communi-cator 4 .05- 4.08, 4.0, 4.5, 4.5BETA, 4.51, 4.6, 4.61, 4.7-4.73; Mozilla Browser M15	The way JPEG images are handled in Netscape Communicator may lead to buffer overflow problems and malicious users running their own code on targeted machines. The browser, mail and news readers are all vulnerable to this.	Upgrade to Netscape 4.74 or Mozilla M16, or newer.	Netscape Communicator JPEG-Comment Heap Overwrite	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
NetZero[35] Windows 95/98/NT 4.0/2000	ZeroPort 3.0 and previous	The username and password are stored locally in a text file called id.dat and inadequately encrypted, which could let a malicious user decrypt them.	No workaround or patch available at time of publishing.	ZeroPort Weak Encryption Method	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
NullSoft[36] Windows 95/98/NT 4.0/2000	Winamp 2.64 and previous	A buffer overflow vulnerability exists when an M3U extension called "#EXTINF:" is being handled, which will either crash the application or allow for the execution of arbitrary code.	No workaround or patch available at time of publishing.	Nullsoft Winamp M3U Playlist Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
OReilly Software[37] Windows 95/98/ NT 4.0/2000	WebSite Professional 2.3.18, 2.4, 2.4.9	A buffer overflow vulnerability exists which could allow a malicious user to execute arbitrary code.	Upgrade to version 2.5 available at: http://website.oreilly.com/support/software/wsp2x_updates.cfm	WebSite GET Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
OReilly Software[38] Windows 95/98/ NT 4.0/2000	Website Professional 2.3.18, 2.4, 2.4.9	An unchecked buffer overflow vulnerability exists in the indexing utility, webfind.exe, which could allow a remote malicious user to execute arbitrary code on vulnerable hosts.	Upgrade to version 2.5 available at: http://website.oreilly.com/support/software/wsp2x_updates.cfm	WebSite 'webfind.exe' Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Rainbow Technologies, Inc. [39] Windows 95/98/NT	iKey 1000	A malicious user can login as administrator and access all private information stored on the device with no detection by the legitimate user. The iKey also allows administrator access using the MKEY (Master Key) password.	Rainbow Technologies has issued a public statement saying they are working to better protect the physical security of the iKey 1000 device. http://www.ntsecurity.net/go/load.asp?iD=/security/ikey1.htm	iKey Administrator Access and Data Compromise	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

[34] Bugtraq, July 24, 2000.
[35] L0pht Research Labs Security Advisory, L0pht-20000718, July 18, 2000.
[36] Securiteam, July 25, 2000.
[37] Cerberus Information Security Advisory , CISADV000717, July 17, 2000.
[38] Network Associates, Inc. COVERT Labs Security Advisory, COVERT-2000-08, July 19, 2000.
[39] L0pht Research Labs Security Advisory, July 20, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Roxen[40] Unix	WebServer 2.0.X	Two vulnerabilities exist which could allow a local malicious user to gain access to the administrative password of the web server and allow remote malicious users to see the content of a directory.	Patch available at: ftp://ftp.roxen.com/pub/roxen/patches/roxen_2.0.50-http.pike.patch	Roxen WebServer %00 Request File/Directory Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Texas Imperial Software[41] Windows 95/98/NT 4.0/2000	WFTPD 2.34, 2.40, 2.4.1, 2.4.1RC11	A few of WFTPD's implemented FTP commands contain security vulnerabilities. These vulnerabilities range from a simple Denial of Service to revealing sensitive server information. All these vulnerabilities can be exploited remotely, and can be done by an anonymous FTP user.	Update to WFTPD 2.4.1RC12 located at: http://www.wftpd.com/	WFTPD Multiple Vulnerabilities	Low/ Medium	Bug discussed in newsgroups and websites. Exploit scripts have been published.
University of Washington[42] Unix	pop2d 4.46, 4.51, 4.54, 4.55	A vulnerability exists in pop2d, which could let any user, who has a pop account on the machine, view any world or group readable file on the file system.	**Temporary workaround (SecurityFocus):** Disabling the pop2d daemon will eliminate this vulnerability. It is typically executed by inetd, and is configured via the /etc/inetd.conf file.	Pop2d Remote File Read	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Virtual Vision[43]	Virtual Vision FTP Browser 1.0	A vulnerability exists when a request to the CGI script, containing the special directory traversal characters, is submitted which could let a malicious user access any directory on the filesystem.	No workaround or patch available at time of publishing.	Virtual Vision FTP Browser	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
WircSrv[44] Windows 95/NT 4.0	IRC Server 5.0.7s	A vulnerability exists in a command, which is supposed to allow the user to access an MOTD (Message Of The Day), that could allow malicious users to access any file within the permission range of the user running the server.	No workaround or patch available at time of publishing.	WircSrv MOTD Read	Medium	Bug discussed in newsgroups and websites.

[40] Securiteam, July 25, 2000.
[41] BluePanda Vulnerability Announcement, July 21, 2000.
[42] SecurityPortal, 2000-07-14, July 24, 2000.
[43] Bugtraq, July 14, 2000.
[44] Bugtraq, July 13, 2000.

*Risk is defined in the following manner:

High - A vulnerability that will allow an intruder to immediately gain privileged access (e.g., sysadmin, and root) to the system. An example of this would be a vulnerability in which a sequence of instructions is sent to a machine by an unauthorized user and the machine responds with a command prompt.

Medium - A vulnerability that will allow an intruder immediate access to the system that is not privileged access. This allows the intruder the opportunity to continue the attempt to gain root access. An example would be a configuration error that allows an intruder to capture the password file.

Low - A vulnerability that provides information to an intruder that could lead to further compromise attempts or a Denial-of-Service (DoS) attack. The reader should note that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered as a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between July 14 and July 27, 2000, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that hackers/crackers are utilizing**. During this period, 46 scripts, programs, and net-news messages containing holes or exploits were identified.

Date of Script (Reverse Chronological Order)	Script name	Script Description
July 27, 2000	Ippersonality-20000727-2.4.0-test4.tar.gz	The Linux IP Personality patch fools OS detection by changing some characteristics of the network traffic. Among the things that can be changed are the TCP Initial Sequence Number (ISN), TCP initial window size, TCP options (their types, but also their order in the packet), answers to some pathological TCP packets, and answers to some UDP packets.
July 27, 2000	Nview10.zip	NetView Scanner is a suite of three security tools for the system administrator or home user, which scans IP addresses for available Windows File & Print Sharing resources, PortScan scans IP addresses for listening TCP ports, and WebBrute scans web directories that are protected with HTTP authentication, testing the strength of the users' passwords.
July 27, 2000	Winamp.m3u.txt	Technique for exploiting the buffer overflow in Winamp's M3U playlist parser, which could allow the execution of arbitrary code.
July 25, 2000	ArpWorks10.EXE	A Windows utility, which sends customized Arp Announce packets over the network. All ARP parameters, including the Ethernet Source MAC address can be changed. Also features an IP to MAC resolver, subnet MAC discovery, host isolation, packets redirection, and IP conflict packets.
July 25, 2000	CISADV000718.txt	Exploit for O'Reilly's WebSite Pro buffer overflow vulnerability, which could allow the execution of arbitrary code.
July 25, 2000	FS-072500-7-ANA.txt	Several DoS exploits for the AnalogX Proxy v4.04 multiple buffer overflow vulnerabilities.
July 25, 2000	Inflex-0.1.5c.tar.gz	An e-mail scanner which scans both incoming and outgoing email without altering your /etc/sendmail.cf file. It can scan for e-mail viruses, unwanted file types (eg., EXE, COM, BMP, MPEG) and file names (eg., stages.exe). It can also be used to scan for text snippets within e-mails.

Date of Script (Reverse Chronological Order)	Script name	Script Description
July 25, 2000	**l0pht.00-07-18.netzero**	**Proof of concept code for the ZeroPort Weak Encryption Method vulnerability.**
July 25, 2000	**l0pht.00-07-20.ikey**	**Proof of concept tool, iSpy, which exploits the Rainbow Technologies' iKey Administrator Access and Data Compromise vulnerabilities.**
July 25, 2000	OW-002-netscape-jpeg-r1.tar.gz	Linux/x86 exploit script for the Netscape Communicator JPEG-Comment Heap Overwrite vulnerability.
July 25, 2000	SA2000-02.ism.dll	Exploit description for the Microsoft IIS v4.0 and 5.0 for Windows NT and Windows 2000 vulnerability, which exposes the contents of .asp, .asa, and .ini files.
July 25, 2000	Saint-2.1.2.beta1.tar.gz	A security assessment tool based on SATAN.
July 25, 2000	Vlad-0.7.tgz	A freeware, open-source scanner that checks for common security problems. VLAD checks for the items referenced in the SANS Top Ten list of common security problems, found at http://www.sans.org/topten.htm.
July 24, 2000	Crash-netscape.jpg	Exploit for the Netscape Communicator JPEG-Comment Heap Overwrite vulnerability.
July 24, 2000	Fawx2.c	Script which sends fragmented junk to port 139, causing a blue screen under Windows 95 / 98 / 2000.
July 24, 2000	Pasvagg.pl	A Perl proof-of-concept exploit for downloading other user's files from FTP servers without needing authentication.
July 24, 2000	PhpDistributedPortScanner-1.0pre1.tar.gz	A Web-based distributed TCP portscanner, which uses plain PHP to perform distributed portscans against a single host.
July 24, 2000	**Wftpd241-11.tgz**	**Perl exploit scripts for the WFTPD/WFTPD Pro 2.41 RC11 four remote Denial of Service vulnerabilities.**
July 22, 2000	Kmap-0.7.2.tar.gz	A QT/KDE front-end to nmap, a popular and powerful console portscanner.
July 22, 2000	Tcpip_lib.zip	A library for Windows 2000 which allows arbitrary packet creation.
July 21, 2000	Sara-3.1.5.tar.gz	A security analysis tool based on the SATAN model.
July 21, 2000	Twwwscan04.zip	A Windows based www vulnerability scanner, which looks for 209 www/cgi vulnerabilities .
July 21, 2000	Wftpdrest.pl	Perl script which exploits WFTPD's multiple vulnerabilities
July 21, 2000	Wftpdrnlst.pl	Perl script which exploits WFTPD's multiple vulnerabilities
July 21, 2000	Wftpdstat.pl	Perl script which exploits WFTPD's multiple vulnerabilities.
July 21, 2000	Wn-ex.c	Remote exploit script for the wn webserver for Linux version v2.0.9 and below buffer overflow vulnerability.
July 21, 2000	Wu-ftpd-v2.4.4.c	Wu-ftpd v2.4(4) remote root exploit script, which exploits the SITE EXEC buffer overflow vulnerability.
July 21, 2000	Xpbitchx.c	BitchX (75p3/1.0c16) local exploit.
July 21, 2000	Xppnc.c	PNC Bouncer remote exploit against v1.11 on RedHat 6.0, SuSE 6.3, and Mandrake 6.0.
July 20, 2000	Dune_poc.c	Script which exploits the Dune Webserver v0.6.7 remote buffer overflow vulnerability.
July 20, 2000	Outoutlook.exe	Exploit for the Microsoft Malformed E-mail Header vulnerability.
July 20, 2000	Outoutlook.pl	Perl script which exploits the Microsoft Malformed E-mail Header vulnerability.
July 20, 2000	Statd-toy.c	Script which exploits the Multiple Vendor Rpc.statd Remote Format String Stack Overwrite vulnerability.
July 19, 2000	Labs50.txt	Exploit script for the Microsoft Outlook vulnerability.
July 19, 2000	Outlook.advisory.txt	Proof of concept exploit for the Microsoft Outlook vulnerability.

Date of Script (Reverse Chronological Order)	Script name	Script Description
July 19, 2000	Outoutlook.zip	Unix Perl version and windows source / binary exploit script for the Outlook Express 5.0, Outlook 2000, Outlook 97.0, and Outlook 98 vulnerability.
July 18, 2000	gkwarez.class	Script which exploits the Gatekeeper Buffer Overflow vulnerability.
July 18, 2000	gkwarez.java	Script which exploits the Gatekeeper Buffer Overflow vulnerability.
July 18, 2000	**Netzero.c**	**Exploit script for the ZeroPort Weak Encryption Method vulnerability.**
July 18, 2000	Wu-ftpd26.c	Remote root exploit for Wu-ftpd 2.6.0 from the ports collection running on FreeBSD v3.3, 3.4 and 4.0.
July 15, 2000	7350qpop.c	Remote exploit script for the qpopper 2.53 euidl x86/linux vulnerability.
July 15, 2000	Directory-URL.prediction.doc	Methods for exploiting Directory and URL Prediction vulnerabilities.
July 15, 2000	Libpcap-0.5.tar.gz	Libpcap is a portable packet capturing library based on the BSD packet filter (BPF). It is very useful for writing sniffers and network analyzers.
July 15, 2000	Md5bd.c	A shell server/backdoor that uses a md5 encrypted password to authenticate, therefore the password cannot be retrieved from the server.
July 15, 2000	Mw-exp.c	Script which exploits the makewhatis local Denial of Service vulnerability.
July 15, 2000	Sscc.tar.gz	Sscc.tar.gz scans C source code for common insecure functions, which can be exploited for buffer overflows. It finds and identifies the file name and line of the possible insecure function.

Script Analysis

When available, this section will supply a short description of scripts that have been analyzed by various security professionals and organizations. **We encourage you or your organization to contribute.** If you wish to do so, please send e-mail to nipc@fbi.gov with the subject line "CyberNotes Script Analysis." While space constraints may limit the length of descriptions included in this document, contributors are requested to include a full technical analysis of the script along with release instructions. The release categories are: releasable to anyone; limited releasability (originator-defined list of organizations); or provided for NIPC only. A member of the CyberNotes editorial team will contact you. All contributions will be credited to the contributing individual or organization unless otherwise requested.

No scripts were submitted during the two-week period covered by this issue of CyberNotes.

Trends

DDoS/DoS:

- An exploit/DoS tool named "octo" or "octopus" has the ability to shut down services remotely. This program opens as many sockets with a remote host as can be supported by both. Often, a remote workstation can be severely disabled by saturating its process table via multiple invocations of sendmail.
- A steady number of reports of intruders using nameservers to execute packet-flooding Denial of Service attacks.

Probes/Scans:

- An increase in scans on port 21 (when WuFTPD 2.5.0 was shown vulnerable).
- An increase to port 543/tcp (Kerberos authenticated services buffer overflow vulnerability).
- A continuation of scans to port 109 (pop2 exploit).
- A continuation of probes to UDP Port 137 (NetBIOS Name Service).
- Additional discussion concerning the AMDROCKS BIND exploit.
- Increasing reports of scans to known Trojan ports. System administrators should consult their intrusion detection system and firewall logs for unusual port scans.

Other:

- **Chat clients and Internet Relay Chat (IRC) networks pose a serious security risk due to recent viruses like the "I Love You" and "Life-Stages" bugs. Both were programmed to take advantage of instant messaging software and chat rooms to spread themselves rapidly across computers and flaws in chat client software and could be easily exploited by malicious users to plant and launch malicious code in corporate networks. Users could be also tricked into communicating sensitive information or downloading files containing malicious code via chat clients.**
- An increase in sites being probed or root compromised related to input validation vulnerabilities in many FTP databases.
- There have been a number of recent malicious programs exploiting the default behavior of Windows operating systems to hide file extensions from the user. This behavior can be used to trick users into executing malicious code by making a file appear to be something it is not. Multiple e-mail-borne viruses are known to exploit the fact that Microsoft Windows operating systems hide certain file extensions.
- A steady number of reports of intruders exploiting unprotected Windows networking shares.
- Reports indicate domain name registration information continues to be maliciously altered, including point of contact information for domain names, IP address delegations, and autonomous system numbers.

Viruses

Natas.4988 (Multipartite and Polymorphic Virus): This virus infects the boot sector of the hard disk (Master Boot Record) and uses stealth techniques. It is activated on executing a previously infected file, at which moment the virus proceeds to overwrite the first sectors of the hard disk and infect other EXE, COM and OVL files. The most evident symptom of infection is an ASCII character string present in all files containing the virus.

PE_Ghostdog2 (Aliases: GHOSTDOG2) (File Infector Virus): This direct infector virus, which was written in Visual Basic, changes the icon of an infected program. Upon executing the virus or infected file, two messages with the title "GhostDog2" are displayed. The virus has no destructive payload and only replicates.

PE_Smash (Aliases: SMASH) (File Infector Virus): This virus overwrites the IO.SYS with 310 bytes causing the system to display the following string upon boot up: "Formatting hard disk … " and then the system hangs up. Once the system is infected and is restarted, another message is displayed. The virus is triggered when the current system date is 14 and month is June or above.

WM97/Bablas-AB (Word 97 Macro Virus): This is a macro virus which disables access to the VB editor, and also prevents the user from closing files without exiting Word.

W97M_Bablas.U (Word 97 Macro Virus): This is a macro virus that infects Word documents and templates when an infected document is closed or opened. It carries a payload that displays message boxes and replaces Word modules on Sundays and Fridays if the time is earlier than 9 PM.

WM97/Eight941-J (Word 97 Macro Virus): This is a macro virus, which only replicates itself.

W97M/Eight941.O1 (Word 97 Macro Virus): This macro virus infects documents which are open and the Microsoft Word global template upon being activated (on July 1st and November 10th) by locating all Microsoft Word documents in the hard disk.

WM97/FF-E (Word 97 Macro Virus): This is a macro virus, which makes changes to MSDOS.SYS to stop Windows 95/98 booting up correctly.

WM97/FF-F (Word 97 Macro Virus): This is a macro virus, which makes changes to MSDOS.SYS to stop Windows 95/98 booting up correctly.

WM97/InAdd-D (Aliases: W97M/Timeless) (Word 97 Macro Virus): On 28th May the virus clears the setting for the 'sTimeformat' Registry key in 'HKU\.Default\Control Panel\International'. The virus also changes the UserName for Word to 'Timeless Phenomenon'.

WM97/Marker-DG (Word 97 Macro Virus): There have been several reports of this virus in the wild. It is a variant of the WM97/Marker Word macro virus. The payload functions if the date is later than 23rd July. When an infected document is opened a message box is displayed:

Did You Wish Shankar on his Birthday ?

When an infected document is closed the Word caption is becomes:

Happy Birthday Shankar-25th July. The world may Forget but not me.

And a message box is displayed:

Did You Wish Jananee on her Birthday ?

If the user selects "Yes" the following message is displayed:

Thank You! I Love You. You are Wonderfull.

If the user answers "No" the following message is displayed:

You are HeartLess. You Will Be Punished For This.

WM97/Marker-EI (Word 97 Macro Virus): This virus appears to be a merging of the WM97/Class-D and WM97/Marker-O viruses. It is a destructive macro virus that infects documents and templates upon closing the target file. This virus carries a payload that triggers when the Visual Basic Editor is invoked on the 15th of any month. The payload deletes the command bars “FILE-PAGE SETUP...", "FILE-PRINT PREVIEW", "FILE-PRINT...", "FILE-EXIT" , "FILE-NEW...", "FILE-OPEN..." and "FILE-CLOSE".

WM97/Marker-ET (Word 97 Macro Virus): This virus is a variant of the WM97/Marker Word macro virus. If the date is later than the 23rd July the virus changes the Word caption to "Happy Birthday rajesh-1st Sept. The world may Forget but not me" and displays a message box. If the user selects "Yes" the following message is displayed:

Thank You! I Love You. You are wonderfull.

If the user answers "No" the following message is displayed:

You are Heart Less

You Will De Punished For This.

W97M_Newhope.H (Word 97 Macro Virus): This is a cleanable macro virus that does nothing but infect other Word documents and templates when a document is opened (Document_Open), closed (Document_Close), or created (Document_New).

WM97/Onex-E (Word 97 Macro Virus): There is a 1 in 75 chance that the virus will attempt to delete the file C:\winnt\system32\ntoskrnl.exe if the system is infected.

WM97/Panther-B (Aliases: Panther.N) (Word 97 Macro Virus): This is a Word macro virus which uses the variable name "HappyPanther." It uses different variable names in documents and the template in an attempt to avoid detection.

XM97/Divi-K (Excel 97 Macro Virus): This virus is an Excel spreadsheet macro virus which creates a file called 874.XLS in the Excel template directory, and will infect other spreadsheets as they are opened or closed. The virus adds a flag, in the form of a variable called IVID plus a hexadecimal number, to each file as it is infected. The virus uses this flag to determine whether the spreadsheet has already been infected.

XM97/Divi-Q (Excel 97 Macro Virus): This virus is an Excel spreadsheet macro virus, which creates a file called SCHEDULE.XLS in the Excel template directory, and will infect other spreadsheets as they are opened or closed. The virus adds a flag, in the form of a variable called IVID plus a hexadecimal number, to each file as it is infected. The virus uses this flag to determine whether the spreadsheet has already been infected.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. The increasing number of Trojans gains added significance due to past reports of anti-virus products not detecting some Trojans or their variants. Readers should contact their anti-virus vendors to obtain specific information on Trojans that their software detects.

The following table provides the reader with a list of Trojans that have received write-ups in CyberNotes. This table includes Trojans discussed in the last four months, starting with CyberNotes #2000-07, and will be updated on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. NOTE: At times, Trojans may contain names or content that may be considered offensive.

Trojan	Version	Issue discussed
Acid Shiver + lmacid	v1.0 + 1.0Mod	CyberNotes-2000-07
Asylum + Mini	v0.1, 0.1.1, 0.1.2, 0.1.3 + 1.0, 1.1	CyberNotes-2000-10 CyberNotes 2000-12
AttackFTP		CyberNotes-2000-10
BF Evolution	v5.3.12	CyberNotes-2000-10
BioNet	v0.84 - 0.92 +2.2.1	CyberNotes-2000-09 CyberNotes 2000-12
Bla	1.0-5.02, v1.0-5.03	CyberNotes 2000-09
Bobo	v1.0 - 2.0	CyberNotes-2000-09
Donald Dick 2		**Current Issue**
Drat	v1.0 - 3.0b	CyberNotes-2000-09
GIP		CyberNotes-2000-11
Golden Retreiver	v1.1b	CyberNotes-2000-10
ICQ PWS		CyberNotes-2000-11
ik97	v1.2	CyberNotes-2000-07
InCommand	1.0-1.4, 1.5	CyberNotes-2000-09
Infector	v1.0 - 1.42, v1.3	CyberNotes-2000-09, CyberNotes-2000-07
iniKiller	v1.2 - 3.2, 3.2 Pro	CyberNotes-2000-09, CyberNotes-2000-10
Kaos	v1.1 - 1.3	CyberNotes-2000-10
Khe Sanh	v2.0	CyberNotes-2000-10
Magic Horse		CyberNotes-2000-10
Matrix	1.4-2.0, 1.0-2.0	CyberNotes-2000-09
Multijoke.B		**Current Issue**
Naebi	v2.12 - 2.39, v2.40	CyberNotes-2000-09 CyberNotes 2000-12
NetController	v1.08	CyberNotes-2000-07

Trojan	Version	Issue discussed
NetSphere	v1.0 - 1.31337	CyberNotes-2000-09
Netsphere.Final		**Current Issue**
Nirvana / VisualKiller	v1.94 - 1.95	CyberNotes-2000-07
NoDesk		CyberNotes-2000-14
Omega		CyberNotes 2000-12
Phaze Zero	v1.0b + 1.1	CyberNotes-2000-09
Prayer	v1.2 - 1.5	CyberNotes-2000-09
Prosiak	beta - 0.65 – 0.70 b5	CyberNotes-2000-09 CyberNotes 2000-12
Revenger	1.0-1.5	CyberNotes 2000-12
Serbian Badman		CyberNotes 2000-12
ShitHeap		CyberNotes-2000-09
Snid	1-2	CyberNotes 2000-12
SubSeven	V1.0-1.9b, v2.1+SubStealth, v2.2b1	CyberNotes-2000-07
Troj/Simpsons		CyberNotes-2000-13
Troj_Dilber		CyberNotes-2000-14
W32.Nuker.C		CyberNotes-2000-14
Win.Unabomber		CyberNotes-2000-14
WinCrash	Beta	CyberNotes-2000-12
Winkiller		CyberNotes 2000-12

Donald Dick 2: A new, redesigned version of the remote administration Trojan Donald Dick reportedly will be coming out soon, possibly in August. Called Donald Dick 2 or Donald Dick Reincarnation, creators of this Trojan say that it will incorporate aspects of the original Trojan as well as new features. Additionally, a commercial version of Donald Dick 1.55 is being advertised now that claims to avoid antivirus programs by utilizing custom features unique to each customer.

Netsphere.Final: This is a Trojan horse that permits invading the systems of computers it has managed to infect. To do so, it uses a file whose icon is typical of an installation program. On being executed, this Trojan horse installs a file named EPP32.EXE in the C:\WINDOWS\SYSTEM folder. When this file is executed, it makes changes to the Windows Registry in order to ensure its presence every time the victim computer is started.

Multijoke.B: This Trojan's only objective is to perform annoying actions on the infected computer. Some of these include opening applications without the user's authorization or interchanging functions of the mouse buttons. The most obvious symptom of infection is the execution of Note Pad. Here it creates a new file within which it inserts a sentence that looks as if it has been typed in via the keyboard.

The Trojan uses any of the regular means of virus propagation to spread; for example disk storage devices (floppy disks, CD-ROMs, other types of devices, etc.), Internet downloads, sending and receiving e-mails with infected attachments, etc.